

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-v-

JATIEK SMITH, ET AL.

Defendants.

22-cr-352 (JSR)

OPINION AND ORDER

JED S. RAKOFF, U.S.D.J.:

By "bottom line" Order dated 3/17/23, the Court denied certain pretrial motions filed by several defendants in this case. See Order, Dkt. 183. This Opinion and Order reaffirms those rulings and sets forth the reasons therefor.

The most significant motion was the motion to suppress evidence filed by defendant Jatiiek Smith. By way of background, on March 2, 2021, agents of the federal bureau of Customs and Border Protection ("CBP").¹ detained defendant Jatiiek Smith as he returned to Newark airport from Jamaica and forced him to turn over his cellphone and its password. They reviewed the phone manually and created and saved an electronic copy of it as it existed as of that date and time -- all without a search warrant. Weeks later (after they had already begun reviewing the electronic copy), the Government applied for and obtained a search warrant.

¹ All capitalized terms here used refer to the definitions set forth in this Opinion and Order, unless otherwise specified. Also, unless otherwise noted, all internal quotation marks, alterations, omissions, emphases, and citations have been omitted from all cited sources.

Smith argues, first, that this search violated his Fourth Amendment rights. To this much of his motion, the Court agrees. While border agents have very substantial latitude to search a person's body and effects without a warrant or probable cause during a border crossing, the Supreme Court has now made clear that searching the data contained on a person's cell phone is not like searching his body or pockets. Rather, searching a cell phone will often allow law enforcement to learn all there is to know about its owner's past movements, communications, and transactions -- reams of information that differ quantitatively and qualitatively from the sorts of information a person could ever have carried with him before the advent of modern "smart" phones. See Riley v. California, 573 U.S. 373 (2014). Moreover, the vast majority of such information will likely have no connection to the traveler's reasons for crossing the border on a given day. Furthermore, unlike a traveler's luggage or cargo -- which, quite obviously, is not yet in the country at the time the traveler presents herself for inspection at the border and can therefore be stopped from coming in -- the information on that traveler's phone most likely already exists outside the phone (in cloud storage or other backups), such that a border search is far less likely to actually prevent anything unwanted from entering or leaving the country.

For these reasons, copying and searching a traveler's phone during a border crossing bears little resemblance to traditional physical border searches historically permitted without probable cause

under the Fourth Amendment's "border search exception." Rather, such searches extend the Government's reach far beyond the person and luggage of the border-crosser -- as if the fact of a border crossing somehow entitled the Government to search that traveler's home, car, and office. The border search exception does not extend so far.

Nonetheless, that still leaves the question whether to suppress the evidence from such an unlawful search. Here, the Court determines that the "good faith" exception precludes suppression, both because at the time of the search, the agents conducting the search had an objectively reasonable basis for believing that there was legal authority binding on them that authorized such a search and also because the Government ultimately obtained a search warrant to search the phone copy, disclosing all relevant details of the search to a neutral magistrate. For these reasons, further elaborated below, the Court reaffirms its prior denial of Smith's motion to suppress.

I. Factual Background

Smith sought to travel from Newark airport to Jamaica on March 2, 2021, where he was denied entry and sent back to the Newark the same day. Gov't Opp. Ex. A, Affidavit of Special Agent Clark ("Clark Decl.") ¶ 14; Declaration of Jatiek Smith ("Smith Decl.") ¶ 3, Dkt. 160. Homeland Security Investigations ("HSI") agents, along with agents of the Federal Bureau of Investigations ("FBI"), were at this time investigating Smith for his and others' alleged role in a putative conspiracy to control the New York area emergency mitigation services

("EMS") industry² through an EMS company called "First Response". Clark Decl. ¶¶ 7-8; see also Indictment ¶¶ 2-10, Dkt. 2. Without seeking a warrant, HSI and FBI agents requested CPB agents to search Smith upon his return to Newark Airport "pursuant to [their] border search authority." Clark Decl. ¶ 14. There, border agents searched Smith's bag (in which Smith was carrying just under \$10,000 in cash), seized Smith's phone, and demanded his password. Id. Smith claims he repeatedly refused to give his password, relenting only after he was told that "[i]f [he] did not open the phone [he] could be held without charge for as long as it took to open the phone." Smith Decl. ¶ 4. The Government more cryptically represents that "Special Agents . . . requested Smith's passcode, which Smith eventually provided."³ Clark Decl. ¶ 14.

² The "EMS industry" refers to companies that provide clean-up services following fires and often also play a role in referring "adjusters" who process fire-related insurance claims. Indictment ¶¶ 1-4.

³ Smith has not argued that the Government, in holding him at the airport until he turned over his phone password, subjected him to a custodial interrogation under Miranda v. Arizona, 384 U.S. 436 (1966). Even if Smith had made a Miranda argument, however, the Court concludes it would not have mattered. Assuming Smith's interrogation was custodial -- something the Court cannot easily determine on this limited record -- Miranda does not require the exclusion of physical evidence obtained based on a suspect's unwarmed but voluntary statements. See United States v. Patane, 542 U.S. 630, 637-42 (2004) (plurality opinion); id. at 644-45 (Kennedy, J., concurring in the judgment). Further still, even if one assumes that Smith's divulging his password was not just unwarmed but also coerced, that would still likely not require suppression. Although courts and commentators have taken varying views on the matter, see Orin Kerr, Compelled Decryption and the Privilege against Self-Incrimination, 97 Tex. L. Rev. 767 (2019), the Court holds the view that being made to produce a phone password -- at least, where, as here, there is no real dispute that

After receiving Smith's passcode, HSI agents made a forensic copy of the phone and returned the original to Smith. Id. In subsequent days, HSI agents began to review the digital copy -- finding, for instance, "communications in which the user of the phone identifies himself as a member of the Bloods and discusses Bloods gang activity," as well as "discussions of Smith's work with First Response, including communications in which he discusses his remuneration arrangement and the 'rules' about responding to fires, as well as communications with what appeared to be either insureds or public adjusters about submitting fraudulent insurance claims." Id. ¶ 15. They also turned over the digital copy to a different group of HSI agents who, in partnership with the FBI, also began reviewing it. Gov't Opp. at 3, Dkt. 168.

Thirty-eight days later (well into multiple law enforcement agencies' review of the digital copy), the Government applied for a warrant to search the forensic copy. See generally Clark Decl.; Gov't Opp. at 3-4. The declaration supporting its application described the airport border search, including that the phone was seized without a warrant "pursuant to HSI's border search authority," and that HSI

the person in fact owns the phone and knows its password -- does not violate the Fifth Amendment's guarantee against self-incriminating testimony. Id. This is because the Fifth Amendment does not prevent compelled production of previously created incriminating evidence where the act of production does not itself involve any incriminating testimony, or where any implicit testimony included in such act of production -- such as acknowledgement of ownership -- can be proved independently. Fisher v. United States, 425 U.S. 391, 411 (1976).

agents copied the phone's contents and had already begun actively reviewing them. Clark Decl. ¶ 14-15. The declaration also relied in part on evidence from this review -- describing, for example, Smith's communications discussing 'rules' imposed on other EMS companies or the submission of false insurance claims. Id. The declaration also included other evidence that might support a search of the phone, such as witness descriptions of a person named "Teak" (whose description corresponded to Mr. Jatiiek Smith's) taking over an EMS company named First Response and proceeding to use violence to set up a "rotation" system through which job assignment in the EMS industry would be shared between companies. Id. ¶ 10. Based on this declaration, Magistrate Judge Aaron issued a search warrant. Clark Decl. at 10 (USAO-000332). The Government's review of the digital copy of Smith's phone continued following the issuance of that warrant. Gov't Opp. at 5.

Six months later, the Government applied for a Title III wiretap on Smith's phone (the same one that had been copied at the border and later searched pursuant to Magistrate Judge Aaron's warrant), as well as the phone of Smith's co-defendant Sequan Jackson. The affidavit in support of the wiretap included evidence from the search of Smith's cellphone, such as excerpts from a WhatsApp conversation between Smith and several of his co-defendants explicitly discussing the "rules" imposed on the industry and the need to discipline other EMS companies that did not follow the "rules". Jackson Ex. A, Clark Affidavit in Support of Wiretap Application ("Clark Wiretap App.") at 15-19. It also included "extensive information provided by witnesses, including

accounts from four victims who had been assaulted and/or extorted by First Response," "toll analyses showing that the conspirators communicated with each other, and with victims, by using cell phones," "information from a confidential source," "results from a warrant on Smith's Facebook account, which showed that Smith was publicly advertising his membership in the Bloods gang," and "analyses of financial records, which showed how some of the defendants were paid (either directly or to related corporations) by First Response." Gov't Opp. at 5; Gov't Ex. B at 20-24, 38-42, 47-48, 51-52. Judge Liman, sitting in Part I, authorized the wiretap of Smith's cellphone as well as of his co-defendant Sequan Jackson, which was then extended for one month following a second application and affidavit detailing, among other things, results from the wiretap so far. Gov't Opp. at 5-6; Gov't Ex. C.

II. Smith's Motion to Suppress

Smith moved to suppress both the phone search and the wiretap, on the grounds that they resulted from the border search. That search, Smith contended, violated his Fourth Amendment rights.

A. Probable Cause Was Required to Search Smith's Phone

The Fourth Amendment provides: "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amdt. IV. As its text

makes clear, the “ultimate touchstone . . . is reasonableness[.]” Brigham City v. Stuart, 547 U.S. 398, 403 (2006). “[W]here a search is undertaken by law enforcement to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant.” Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995). This “ensures that the inferences to support a search are drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.” Riley v. California, 573 U.S. 373, 382 (2014). “In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.” Id.

Smith argues that the warrantless search of his cell phone at Newark airport violated his Fourth Amendment rights. To evaluate this argument, this Court must weigh two different strands of precedent: one that gives the Government exceptionally broad authority to effect warrantless searches or seizures at the border (usually without any kind of heightened suspicion), see II.B.1, infra, and a newer line of cases concerning one’s Fourth Amendment rights applicable to the vast quantities of sensitive data stored on electronic devices such as cell phones, see II.B.2, infra. The Court summarizes each line of cases, before analyzing how they interact here. See I.B.3, infra.⁴

⁴ Smith also argues that the border search exception is not even implicated because, since he was denied entry to Jamaica, he did not actually cross any border. Smith Mem. 9, Dkt. 161. The Court disagrees. The fact that Smith was denied entry to Jamaica does not change the fact that the search occurred after Smith had just arrived on a plane from Jamaica and was seeking to reenter the United States. Whether

1) The Border Search Exception

One “exception” to the ordinary requirement that the Government first obtain a warrant before conducting a search relates to border searches. Such searches, “pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border” United States v. Ramsey, 431 U.S. 606, 616 (1977). Citing a customs statute passed by the First Congress that granted customs inspectors the “full power and authority” to search “any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed,” id. at 616 (quoting the Act of July 31, 1789, c. 5, 1 Stat. 29), the Ramsey Court reasoned that “[b]order searches, then, from before the adoption of the Fourth Amendment, have been considered to be ‘reasonable’ by the single fact that the person or item in question had entered into our country from outside.” Id. at 619. “The border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country.” Id. at 620.

The border-search exception is not, however, entirely unlimited. For instance, the Supreme Court has applied the “reasonable suspicion” standard to the question of whether the Government may detain someone

Smith was admitted to Jamaica does not change the fact that he plainly left the United States, such that his return involved a border crossing.

at the border suspected to be "smuggling contraband in her alimentary canal" for long enough for that contraband to be passed. United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985). Further, in this and several other circuits, reasonable suspicion is required before the Government may conduct "more personally offensive searches" such as strip searches. United States v. Asbury, 586 F.2d 973, 976 (2d Cir. 1978).

Importantly, these cases make clear that the border is not a totally Fourth Amendment-free zone. Rather, even at the border, "[t]he Fourth Amendment commands that searches and seizures be reasonable," and "[t]he permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests." Montoya, 473 U.S. at 537. What differs at the border is the standard of reasonableness, which plays out in a "qualitatively different" way "at the international border [versus] the interior." Id. at 538.

2) Cell Phones and Riley v. California

Neither the Second Circuit nor the Supreme Court has addressed how, if at all, the border search exception applies to the content of a person's digital cell phone.⁵ However, the Supreme Court has provided

⁵ By "cell phone," the Court means the digital "smartphones" owned by 85% of U.S. adults. Pew Research Center, Mobile Fact Sheet, <https://www.pewresearch.org/internet/fact-sheet/mobile/>. That such devices act as conventional telephones is almost incidental. They are pocket-size computers that many adults (and non-adults) carry with them at all times and through which they send texts and emails, buy products, navigate to and from destinations, watch entertainment, consume news, participate in social media, search the Internet, take

guidance as to how to think about the problem. Specifically, Riley v. California, 573 U.S. 373 (2014), in considering the warrant exception allowing warrantless searches pursuant to a lawful arrest, the Supreme Court did not automatically extend the exception to searches of cell phones' digital data. It instead analyzed whether the logic behind the warrant exception applied to cell phone searches. Id. In so doing, the Court made clear its awareness that modern cell phones are materially different from the other types of objects a person might carry because they contain huge quantities of often highly personal data that could not previously have been contained in a pocketable object. Id. at 393.

Specifically, to determine whether the rationale for the search-incident-to-arrest exception in fact applied to cell phone searches, the Supreme Court "assess[ed], on the one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." Id. at 385 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)). This "balancing of interests" (which forms the basis for the search-incident-to-arrest exception itself, id. at 386⁶) allows warrantless searches of an arrestee's person and pockets so as to ensure officer safety, prevent escape, and safeguard evidence in light of the arrestee's "reduced privacy interests upon being taken

and post photographs and videos, and -- occasionally -- make phone calls.

⁶ The same "balancing of interests" underlies the border search exception. See II.B.1, supra; Montoya, 473 U.S. at 537-38.

into police custody." Id. at 391. However, this same balancing had long meant that the exception did not permit warrantless searches of the arrestee's house, which did not implicate the same state interests and would represent "a substantial invasion [of privacy] beyond the arrest itself" Id. at 392 (citing Chimel v. California, 395 U.S. 752, 766-67 (1969)).

So too with cell phones. The Court in Riley held that the arresting officer's interest in searching an arrestee to remove dangerous items did not apply to cell phones because "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape." Id. at 387. Similarly, the government's interest in preventing the destruction of evidence did not support allowing warrantless cell phone searches because, instead, law enforcement could prevent any destruction of digital evidence by turning off the phone, disconnecting it from networks, or placing it in a device meant to secure it from remote wiping until a warrant could be obtained. Id. at 390-91. Further, and perhaps most crucially, an individual's privacy interest in his cell phone differed fundamentally from that same individual's privacy interests with respect to his person or the contents of his bags or pockets. Id. at 393. This was because "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of" the other sorts of physical items a person might carry in her pocket. Id. Indeed, the Court treated with near scorn the Government's argument "that a search of all data stored on a cell

phone is ‘materially indistinguishable’ from searches of these sorts of physical items,” calling that argument “like saying a ride on horseback is materially indistinguishable from a flight to the moon.” Id. Instead, the Court made clear that “[a] conclusion that inspecting the contents of an arrestee’s pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.” Id.

Such an extension, the Court held, failed because the data contained on an arrestee’s phone “differ[s] in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person.” Id. at 393. While “[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read[,] nor would they have any reason to attempt to do so . . . the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones.” Id. at 393-94. Further, “a cell phone collects in one place many distinct types of information -- an address, a note, a prescription, a bank statement, a video -- that reveal much more in combination than any isolated record.” Id. at 394. And cell phones’ enormous storage capacity “allows even just one type of information to convey far more than previously possible,” such that “[t]he sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved

ones tucked into a wallet." Id. Moreover, "the data on a phone can date back to the purchase of the phone, or even earlier," including records of calls and written communications dating back months or years that almost certainly would never be contained in non-digital papers found on a person. Id. And "[f]inally, there is an element of pervasiveness that characterizes cell phones but not physical records." While "[p]rior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day," it is now "the person who is not carrying a cell phone, with all that it contains, who is the exception." Id.

Further still, the kinds of data stored on a cell phone makes them "qualitatively different" from the sorts of physical records or objects a person might carry with them. Id. A person's "Internet search and browsing history" might "reveal an individual's private interests or concerns," such as private medical details. Id. at 395-96. Also, "[h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." Id. at 396. These were just some of the many kinds of highly private data many or most users might have stored on their phone. Id.

Lest there be any doubt, the Court in Riley noted that while it had previously echoed Judge Learned Hand's 1926 observation "that it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him' . . . [i]f his pockets contain a cellphone,

however that is no longer true." Id. Instead, a "cell phone search would typically expose to the government far more than the most exhaustive search of a house: [a] phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form -- unless the phone is." Id. at 396-97.

3) Cell Phones at the Border

Although Riley itself concerned searches incident to lawful arrests, its logic would seem to apply to cell phone searches at the border. Specifically, as in Riley, a court should decide "whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'"⁷ Id.

⁷ Riley did include a potential caveat to any need for such a balancing inquiry: specifically, where there is "precise guidance from the founding era," such guidance might resolve the need for a warrant. Id. at 385. See also United States v. Jones, 565 U.S. 400, 406-07 (2012) (looking to the original understanding of the Fourth Amendment to determine whether the physical trespass involved in placing a GPS device on a person's car constituted a search or seizure). It is certainly true that courts have grounded the border search exception in historical understanding. Ramsey, 431 U.S. at 616 (discussing a customs statute passed by the First Congress as probative of the Fourth Amendment's application to border searches). However, as discussed above, Riley made clear that courts could not simply extend historical acceptance of warrantless searches of physical items at a particular time or place to phones; rather, the unique qualitative and quantitative differences between the sort of information contained on cell phones and that contained in physical records requires consideration of whether the logic behind a historically grounded exception applies to cell phones. Riley, 573 U.S. at 393-403. See also Orin Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J.L. & Pub. Pol'y 403 (2013) (arguing for "[t]he need for different

at 385. In conducting this analysis, courts should not automatically presume that a balance previously struck as to a certain kind of physical search automatically extends to a search of the data contained on a person's cell phone. *Id.* at 393. Rather, courts should independently evaluate whether the governmental interests thought to support a warrant exception actually apply to cell phone searches, and whether the intrusion on privacy posed by a physical search is relevantly comparable to that posed by a search of cell phone data. See *id.* at 385-403. See also United States v. Aigbekaen, 943 F.3d 713, 720 (4th Cir. 2019) ("[A] warrant exception will not excuse a warrantless search where applying the exception would untether the rule from the justifications underlying it."). Application of Riley at least this far should prove uncontroversial, as the Supreme Court has indicated that the border search exception is itself the product of precisely this kind of balancing of interests. Montoya, 473 U.S. at 538-39.

Applying this balancing framework to phone searches at the border yields the same result as in Riley. None of the rationales supporting the border search exception justifies applying it to searches of digital information contained on a traveler's cell phone, and the

rules governing digital devices"); Note, *The Border Search Muddle*, 132 Harv. L. Rev. 2278, 2287-99 (2019) (arguing that it remains unclear how the founding generation thought about border searches as applied to a person's papers, such that applying the border search exception to the contents of a cellphone necessarily requires legal reasoning beyond historical description).

magnitude of the privacy invasion caused by such searches dwarfs that historically posed by border searches and would allow the Government to extend its border search authority well beyond the border itself. As such, the Court concludes that the Government may not copy and search an American citizen's⁸ cell phone at the border without a warrant absent exigent circumstances.

In reaching this conclusion, the Court first considers, as in Riley, the governmental interests previously relied upon to support the warrant exception urged here. Border-search cases often refer at a fairly general level to the Government's interest in "the protection of the integrity of the border," which of course includes the Government's interests in preventing the introduction into this country of illicit substances or contraband. Montoya, 473 U.S. at 536-38. The Government's interests also include apprehending persons who may pose a threat or who lack authorization to be present in this country, United States v. Martinez-Fuerte, 428 U.S. 543, 556 (1976), in inspecting goods to ensure appropriate customs tax is paid, Ramsey, 431 U.S. at 616, and more generally "protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives." Montoya, 473

⁸ The Court need not here address whether the same result would hold for a non-resident or non-citizen. Cf. United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990) (holding that the Fourth Amendment does not protect property held in Mexico by a Mexican resident and citizen against search or seizure by the U.S. Government).

U.S. at 544. In other words, the Government has a very strong interest in preventing unwanted persons or items from entering the country.

But despite the strength of this interest, it is hard to see how it applies to searches of the digital data contained on a traveler's cell phone. When the Government interdicts contraband, identifies goods subject to customs tax, or prevents someone from entering the country without authorization, it successfully stops a person or thing outside the country from unlawfully coming into it. But data stored on a cell phone is not like that -- it instead can and very likely does exist not just on the phone device itself, but also on faraway computer servers potentially located within the country. And, wherever the servers are located, the owner of a cell phone can generally access or share part or all of the data on it with anyone else in the world so long as both parties have an internet connection. Stopping the cell phone from entering the country would not, in other words, mean stopping the data contained on it from entering the country. See, e.g., Orin Kerr & Robert Wisberg, *Searching Computers at the Border*

(Stanford Law School Zoom Event, 3/3/22), <https://www.youtube.com/watch?v=WflaKYW1jUI>. See also Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 365-77 (2015) (discussing the challenges the diffusion of data poses to firm concepts of territoriality).

Some courts have suggested that cell phones might contain so-called "digital contraband" such as explicit images involving the sexual abuse of children. See, e.g., *United States v. Cano*, 934 F.3d

1002, 1014 (9th Cir. 2019) (reasoning that “because cell phones may ultimately be released into the interior . . . the United States has a strong interest in preventing the entry of such material.”). Given what the Court has just discussed about how digital data exists separate and apart from the physical cell phone on which it is stored, the Court doubts that the Government’s interest in interdicting such “digital contraband” as it exists on a specific device -- when the exact same digital contraband likely is already stored outside the device and available to its owner and others within this country -- is genuinely comparable to the Government’s interest in interdicting physical contraband. Physical contraband, once interdicted, will not enter the country, whereas digital contraband easily could and very likely already has. But, in any event, no party seriously contends that the search of Smith’s phone in this case was for “digital contraband,” so the Court need not definitively resolve the precise extent of the Government’s interest in interdicting digital contraband. Cf. id. at 1019-21 (reasoning that while border agents could conduct warrantless forensic searches of phones for digital contraband with reasonable suspicion, they could not conduct warrantless phone searches for anything other than digital contraband). Therefore, while the Court acknowledges the Government’s strong interest in searching persons or physical objects at the border, any corresponding interest in searching the digital data “contained” on a particular physical device located at the border is relatively weak. Kerr & Wisberg, supra at 18:00-20:00.

The Court weighs against this relatively weak governmental interest a citizen's privacy interests in her cell phone data at the time she presents herself at a U.S. border. Just as in Riley, the cell phone likely contains huge quantities of highly sensitive information -- including copies of that person's past communications, records of their physical movements, potential transaction histories, Internet browsing histories, medical details, and more -- that this Court has already addressed at some length. Section II.B.2, supra; Riley, 573 U.S. at 394-97. To be sure, an individual who presents herself at a border crossing has diminished privacy interests because she should reasonably expect that her person or possessions may be subject to search. Montoya, 473 U.S. at 539-40. Similarly, an individual subject to arrest and impending detention has substantially "reduced privacy interest[s] upon being taken into police custody." Riley, 573 U.S. at 391. But, just as in Riley, this kind of reduced privacy interest has always been understood with respect to the physical things a person carried with her -- whether at the time of the arrest or, as here, at the time of a border crossing. Technological and cultural changes now mean that nearly all travelers carry with them, in addition to any physical items, a digital record of more information than could likely be found through a thorough search of that person's home, car, office, mail, and phone, financial and medical records, and more besides. No traveler would reasonably expect to forfeit privacy interests in all this simply by carrying a cell phone when returning home from an international trip. Because the government's interests in a

warrantless search of a cell phone's data are thus much weaker than its interests in warrantless searches of physical items, and a traveler's privacy interests in her cell phone's data are much stronger than her privacy interests in her baggage, the Court concludes that the same balancing test that yields the border search exception cannot support its extension to warrantless cell phone searches at the border.⁹

In holding that warrants are required for cell phone searches at the border, the Court believes it is applying in straightforward fashion the logic and analysis of Riley to the border context. Importantly, however, the Court recognizes that of the five federal courts of appeals to consider the question, none has gone quite this far (although the Ninth Circuit has come close). But it is clear that both the Ninth Circuit and the Fourth Circuit would have required a warrant for the search conducted here.

Specifically, the Ninth Circuit held in 2019 that border officials may conduct warrantless searches of cell phones "only to determine whether the phone contains contraband," such as explicit images of child sexual abuse. Cano, 934 F.3d at 1018. Searches for evidence

⁹ This of course does not mean that under exigent circumstances, the Government could not conduct warrantless phone searches or seizures at the border. Kentucky v. King, 563 U.S. 452, 460 (2011). The Court need not here address whether circumstances that might not qualify as exigent within the country could qualify in the border context. The Court likewise need not address whether the Government may have relatively greater leeway at the border than elsewhere to temporarily seize or copy a phone until it is able to apply for a warrant.

relating to a crime (such as the search here) require a warrant, because the Government's interest in obtaining evidence -- as opposed to interdicting contraband or other unwanted items or persons -- is not materially different at the border than elsewhere. Id. at 1016-19.

As there is no dispute that the search here was not for digital contraband, applying Cano's logic would lead to the same result in this case that the Court independently reaches: that the warrantless search and copying of Smith's phone was unlawful. As to Cano's other holding -- that warrantless searches for digital contraband are permissible, whether without any heightened suspicion in the case of "manual" searches (scrolling through someone's phone), or with reasonable suspicion in the case of more thorough "forensic" searches, id. at 1012-16 -- the Court doubts that the Government's interest in interdicting so-called "digital" contraband is genuinely comparable to its historically grounded interest in interdicting physical contraband, since, as discussed above, digital data is rarely stored uniquely on a cell phone such that seizing such a phone with unwanted data really would mean preventing that data from "entering" the country. However, the Court need not definitively resolve that question, since there is no question that the search here was not for digital contraband.

Applying similar logic to Cano, the Fourth Circuit in United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018) likewise reasoned that a warrantless search of a cell phone at the border is impermissible

absent some nexus between the Government's interests in protecting the border and the search. Id. at 143. However, unlike the Court in Cano, the Fourth Circuit reasoned that such a "nexus" could be satisfied not just by the phone containing actual digital contraband but also by its containing evidence of a border related violation (such as, as in Kolsuz, suspected smuggling of firearms). Id.

As noted by the Cano court, this reasoning effectively enlarges the border search exception, by transforming a warrant-exception based on the Government's interest in preventing the introduction of unwanted persons or things into an interest in "search[ing] for evidence of contraband that is not present at the border." Cano, 934 F.3d at 1018. Of course, whether at the border or elsewhere, the Government has a strong interest in obtaining evidence of illegality, including illegality that may occur at the border. But, just as that interest cannot support the Government's conducting a warrantless search of a person's house simply because it believes it may contain evidence of a crime, it does not support allowing the Government to conduct warrantless searches of cell phones for evidence of border-related crimes. Id. However, notwithstanding this Court's disagreement with the Fourth Circuit's approach, the Court notes that even under that approach, the warrantless phone search conducted here for evidence of crimes having nothing to do with the border would not have been permissible. See United States v. Aigbekaen, 943 F.3d 713, 720-21 (4th Cir. 2019) ("[T]he Government may not invoke the border exception on

behalf of its generalized interest in law enforcement and combatting crime.”).

It is important to note, however, that two other circuit courts to address the question have held that the Government may search cell phones at the border without a warrant and without any heightened requirement of nexus between the search and the Government’s interests in preventing the entry of unwanted persons or items. See Alasaad v. Mayorkas, 988 F.3d 8, 21 (1st Cir. 2021); United States v. Touset, 890 F.3d 1227, 1223 (11th Cir. 2018). Additionally, the Eighth Circuit recently indicated its likely agreement with the First and Eleventh Circuits, although, since the Government’s search in that case sought to uncover evidence of trade secrets being smuggled out of the country, the court declined to definitively resolve whether there is any nexus requirement. United States v. Xiang, 2023 WL 3263857, at *4-6 (8th Cir. 2023 May 5, 2023). In any event, none of these decisions is persuasive to this Court or binding upon it.

The First Circuit sought to distinguish Riley by stating that “[t]he search incident to arrest warrant exception [at issue in Riley] is premised on protecting officers and preventing evidence destruction, rather than on addressing border crime.” Alasaad, 988 F.3d at 21. It further emphasized that the “border search exception’s purpose is not limited to interdicting contraband; it serves to bar entry to those ‘who may bring anything harmful into this country’ . . . [including] ‘communicable diseases, narcotics, or explosives.’” Id. at 20. This Court agrees that the governmental interest underlying the

border search exception is different from that underlying the search-incident-to-arrest exception, and it acknowledges that the former extends to preventing a wide variety of harmful things from entering the country. But, as discussed above, "things" are different from "data", so it is hard to see why the interests underlying the border search exception extend to the data stored on a traveler's cell phone. To be sure, that data may contain information relevant to the Government's determination as to whether a person should be allowed entry, but the Government has little heightened interest in blocking entry of the information itself, which is the historical basis for the border search exception. The Government's more general investigative interest in data about the person or thing entering the country is entirely incidental to the fact of the cell phone being carried over the border, and could just as easily be relied upon to support searches of the person's home, records, or past mail far away from the border.

The Eleventh Circuit, meanwhile, relied heavily on the example previously discussed of "digital contraband" such as explicit sexual material involving minors (which is not surprising, since the case involved a search for such material). Touset, 890 F.3d at 1232-33. Putting aside this Court's previously expressed doubts as to the strength of the Government's interest in preventing the entry of a particular device containing such material -- which, more likely than not, is also stored outside the device and already accessible within this country -- any interest in seizing "digital contraband" would not justify warrantless searches for other purposes, as the Ninth Circuit

made clear in Cano. 934 F.3d at 1018. The Eleventh Circuit meanwhile brushed aside the Supreme Court's reasoning in Riley as concerns the unique privacy implications of cell phone searches, arguing that "it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects" since "[t]he same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents." Touset, 890 F.3d at 1233. The analogy seems weak on its face: relatively few travelers cross the border in an RV or truck with all their personal possessions and documents in store, while this Court surmises that most travelers carry a cell phone. More to the point, as the Supreme Court made clear in Riley, the storage capacity and pervasive use of cell phones in every aspect of users' lives make them qualitatively and quantitatively different from the sorts of possessions or records a person might carry with her. Riley, 573 U.S. at 393. True, the Riley court made that observation in the context of considering the kinds of objects a person might have on their person or perhaps in their car at the time of an arrest, while it might be likely that travelers at the border carry relatively more physical objects with them. But the basic point -- that a cell phone carries far more and far more sensitive information than would historically have been contained in carriable physical objects -- plainly applies at the border as well.

Finally, and quite recently (well after the search in this case), the Eighth Circuit distinguished Riley on the barebones basis that it

"involved a different Fourth Amendment exception, searches incident to arrest," without explaining why the logic of Riley does not apply in the border context. Xiang, 2023 WL 3263857, at *3. As already explained, the Court agrees that Riley does not extend automatically to the border search context, but the Court disagrees that this alone serves to distinguish it. Rather, courts should apply the methodology Riley laid out for evaluating when a warrant exception applies to the data contained on phone searches by balancing the governmental interests supporting the exception against the privacy interests implicated -- the same exact balancing test used to produce the underlying warrant exceptions, Riley, 573 U.S. at 386; Montoya, 473 U.S. at 538-39. Applying that methodology, it seems clear that the border search exception should not extend to warrantless searches of the data contained on cell phones. In any event, the Eighth Circuit did not definitively resolve whether a warrantless border search of a cell phone requires some nexus to a border-related rationale (as held by the Ninth and Fourth Circuits), since it reasoned that the search in that case -- for trade secrets the defendant was suspected of smuggling abroad -- plainly had such a nexus. Id.

For the foregoing reasons, the Court concludes that the warrantless search of Smith's cell phone was unreasonable under the Fourth Amendment. As discussed above, this Court's preferred rule -- that phone searches at the border generally require warrants outside exigent circumstances -- is somewhat more protective than the approach of any circuit court to consider the question. But even under the

approaches of the Fourth and Ninth Circuits, a warrant would have been required to search Smith's phone since this was neither a search for digital contraband nor for evidence of physical contraband. Cano, 934 F.3d at 1018; Aigbekaen, 943 F.3d at 720-21. Thus, whether the Government must obtain a warrant for all border cell phone searches (absent exigent circumstances), or just those border phone searches not immediately connected with preventing unwanted persons or things from entering the country, a warrant was required here.

B. Whether to Suppress the Phone Search

Deciding that the border search of Smith's cell phone was unlawful does not, however, answer whether the results of the search should be suppressed. After all, "[e]xclusion is 'not a personal constitutional right,' nor is it designed to 'redress the injury' occasioned by an unconstitutional search," but rather is meant "to deter future Fourth Amendment violations." Davis v. United States, 564 U.S. 229, 236-37 (2011). Accordingly, while courts will ordinarily exclude evidence obtained in violation of the Fourth Amendment, such evidence may still come in under various exceptions to the exclusionary rule. The Government argues that three such exceptions -- the independent source, inevitable discovery, and good faith exceptions -- are implicated here. The Court discusses each in turn.

1) The search of Smith's phone did not derive from an independent source

The Government first invokes the "independent source" exception, which allows the Government to rely at trial on evidence obtained in

violation of the Fourth Amendment in some circumstances if it can show that it would have obtained the evidence in any event pursuant to a later and lawfully obtained warrant. See Murray v. United States, 487 U.S. 533, 542 (1988). The Government argues that because Magistrate Judge Aaron ultimately issued a warrant to search the electronic copy of Smith's cell phone during the border search, and the affidavit filed in support of its warrant application included information beyond that already found on Smith's cell phone (such as witness accounts describing Smith's conduct), the ultimate search of Smith's phone was based on probable cause independent of the border search. Gov't Opp. at 17-18; Gov't Sur-Reply at 7, Dkt. 181.

The Court disagrees. For the independent source exception to apply, two conditions must hold. First, "the warrant must be supported by probable cause derived from sources independent of the illegal entry." United States v. Johnson, 994 F.2d 980, 987 (2d Cir. 1993). Second, "the decision to seek the warrant may not be prompted by information gleaned from the illegal conduct." Id. Neither condition is met here.

In this regard, the Court disagrees with the Government's claim that the warrant the Government ultimately obtained was "substantially based on information that was untethered to the cursory" search of the phone already performed at the time it sought the warrant. Gov't Opp. at 17. To be sure, the affidavit submitted in support of the Government's warrant application included significant independent evidence of Smith's potentially unlawful conduct, including the

results of witness interviews, information taken from Smith's social media page, and more. However, other than relatively conclusory assertions that evidence of the sort sought generally exists on cell phones, the only specific information indicating that evidence of illegality would likely be found on Smith's phone were descriptions of already-reviewed text messages that indicated Smith's membership in the Bloods gang as well as his role in enforcing "rules" on other emergency mitigation companies as to how to respond to fires. Clark Decl. ¶ 15. As such, the Court seriously doubts that the warrant application stood on its own in establishing probable cause absent the information it contained about the evidence stored on Smith's phone.

More fundamentally, the ultimate search of the forensic copy of Smith's phone could not have been "independent" of the initial unlawful search, because the forensic copy existed only because of that search. Even if the Government had independent probable cause to search Smith's cell phone at the time it obtained its warrant, the search it actually performed was of a copy of Smith's cell phone made during the border search -- a copy that almost certainly contained at least somewhat different data from the actual phone at the later moment when the Government obtained a warrant. Accordingly, the search was plainly not independent of the unlawful border search.

2) The cell phone search was not inevitable.

For similar reasons, the Government cannot rely on the "doctrine of inevitable discovery," which applies when the Government can "establish by a preponderance of the evidence that the information

ultimately or inevitably would have been discovered by lawful means." United States v. Eng, 971 F.2d 854, 859 (2d Cir. 1992). Once again, the difficulty is that because the Government searched a copy of Smith's phone made during the initial search, any later search of that forensic copy -- as opposed to a search of the data contained on Smith's phone at a later point in time -- would not probably have occurred but for the initial unlawful search. See, e.g., Orin Kerr, *The Fourth Amendment Limits of Internet Content Preservation*, 65 St. Lo. L.J. 753, 807 (2021) ("Applying the inevitable discovery exception leads to a simple outcome . . . [i]f the preservation copy is the fruit of an unconstitutional seizure, then it should not have existed and it cannot be used."). Since the copy of Smith's cell phone containing the data existing as of the date and time of the border search would not have existed but for the unlawful search -- and since the data contained on Smith's actual phone as of the time the warrant issued may have materially differed from the data contained on the copy -- the warranted search of the phone copy was not inevitable.

3) The Good Faith Exception

Finally, the Government argues that the good faith exception to the exclusionary rule applies. That exception allows unlawfully obtained evidence to be used at trial "when the Government acts with an objectively reasonable good-faith belief that their conduct is lawful." United States v. Zodhiates, 901 F.3d 137, 143 (2d Cir. 2018). The Government has therefore been allowed to rely on unlawfully obtained evidence where, for instance, "the police conduct a search

in objectively reasonable reliance on a warrant later held invalid," where "searches [are] conducted in reasonable reliance on subsequently invalidated statutes," or where "the police conduct a search in objectively reasonable reliance on binding judicial precedent." Davis v. United States, 564 U.S. 229, 239-40 (2011). Generally, exclusion is appropriate "[w]hen the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights [because] the deterrent value of exclusion is strong and tends to outweigh the resulting costs." Id. at 238. However, "when the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful, or when their conduct involves only simple, 'isolated' negligence, the 'deterrence rationale loses much of its force,' and exclusion cannot 'pay its way.'" Id. at 238.

The Government here offers two good faith arguments: first, that the initial border search, even if unlawful, itself falls under the good faith exception, and second, that the Government's later reliance on Magistrate Judge Aaron's warrant falls under the good faith exception. The Court agrees with both arguments.

i) The Government's initial border search falls under the good faith exception.

As to the first argument, the breadth of the "border search exception" was still largely in place at the time of the search. Indeed, two of four federal circuit courts of appeals that had addressed forensic searches of cell phones at the border had held that such seizures and searches were lawful without warrants independent

of any nexus between the search and a border-related rationale.¹⁰ While two other circuit courts had indicated to the contrary, given the historic breadth of the “border search exception,” a reasonable government agent could have a good faith belief that such a search as was conducted here was permissible absent Supreme Court or Third Circuit precedent to the contrary.

Furthermore, even if that were not enough, a reasonable border agent could have in good faith believed that the search conducted here was expressly warranted by a 2018 CBP directive, which purports to allow so-called “manual” phone searches at the border without any heightened standard of suspicion and “advanced search[es]” -- which entail “connect[ing] external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents” -- whenever “there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP”¹¹ or “when there is a national security concern. . . .” CBP Directive No. 3340-049A at 4-5, U.S. Customs and Border Protection (Jan. 4, 2018), Dkt. 159-1.

“Reasonable suspicion” is, of course, a modest standard requiring much less than the “probable cause” required for a warrant. The

¹⁰ The most applicable circuit (the Third, because the phone was seized at Newark airport) had not addressed the issue at all.

¹¹ The Government represents that Title 18 of the U.S. Code is one of almost 30 titles enforced in some capacity by CBP. Gov’t Opp. at 13 (citing “Summary of Laws Enforced by CBP,” available at <https://www.cbp.gov/trade/rulings/summary-laws-enforced/us-code>).

Government contends there was reasonable suspicion here either because of the information its investigation of Smith's domestic activities had already yielded, or because of the circumstances of Smith's arrival at Newark Airport from Jamaica in March 2021, when he had left Newark earlier that day and been denied entry in Jamaica and was carrying just under \$10,000 in cash. Gov't Opp. at 15. At the very least, the information later presented to Magistrate Judge Aaron in obtaining a warrant clearly indicates that, even prior to the search, the Government had objectively reasonable suspicion of Smith's involvement in criminal activity. The border agents who searched Smith at the express request of the government agents conducting the underlying investigation thus had more than a good faith basis for believing that they were acting under the authority of the 2018 CBP directive in seizing and searching Smith's cell phone.¹²

This conclusion is further reinforced by the Second Circuit's decision in United States v. Levy, 803 F.3d 120 (2d Cir. 2015), in which it held that a CBP agent could search and copy the contents of a traveler's notebook based on reasonable suspicion of the traveler's

¹² Of course, law enforcement agencies cannot launder unconstitutional practices by promulgating internal guidance that does not itself demonstrate an objectively reasonable good faith effort to apply the law, as any "good faith" reliance by line officers on such guidance would depend on the bad faith of their superiors. Here, however, the CBP guidance document, which requires reasonable suspicion for forensic searches, was more protective than what some courts had held to be required, Touset, 890 F.3d at 1233, and reflects an objectively reasonable attempt to apply the law in this unsettled area.

involvement in financial crimes that other government law enforcement agencies were investigating. Id. at 122-24.¹³ There, the Second Circuit rejected the traveler's argument "that border searches conducted by the CBP, even at the prompting of another federal agency, should at least be confined to crimes that a statute or regulation specifically authorizes CBP to investigate," and instead reasoned that "CBP officers are neither expected nor required to ignore tangible or documentary evidence of a federal crime." Id. at 124 (stating that CBP agents "have the authority to search and review a traveler's documents and other items at the border when they reasonably suspect that the traveler is engaged in criminal activity, even if the crime falls outside the primary scope of their official duties"). While Levy is distinguishable from the instant case because it dealt with a physical notebook, rather than a cell phone (which, as discussed extensively above, poses unique privacy concerns, see II.A.2-3, supra), it nonetheless supports the contention that government agents considering the law as it existed at the time of the border search could reasonably believe they had a binding lawful basis for seizing and searching Smith's cell phone.

In short, because the agents who requested the search had objectively reasonable suspicion to so request and the agents who actually conducted the search had what they could have reasonably

¹³ Although the agents who carried out the search at Newark airport were directly subject to Third Circuit law, they were acting at the behest of the New York investigative agents, who were governed by Second Circuit law.

considered as binding authority to do so under the 2018 CBP Directive, the search meets the requirements for the good faith exception to the exclusionary rule.

ii) The Government properly relied on a later-issued warrant

Independent of its conclusion that the good faith exception applies to the Government's initial unlawful phone search, the Court separately concludes that the good faith exception precludes suppression of the fruits of that search because the Government ultimately obtained a search warrant. The core good faith exception to the exclusionary rule applies where the Government reasonably relies on a duly issued search warrant, even if that warrant should never have issued. United States v. Leon, 468 U.S. 897, 913-18 (1984). Here, much (though not all) of the Government's actual search of the copy made of Smith's phone occurred after a search warrant was issued by Magistrate Judge Aaronson. Clark Decl. ¶ 14; Gov't Opp. at 3-4. True, the Government obtained that warrant after the initial search occurred, and in order to establish probable cause, the Government relied in its warrant application on information already obtained (in this Court's view, unlawfully) from Smith's phone. Clark Decl. ¶¶ 14-15. But it disclosed the relevant circumstances of the search -- including that CBP agents seized, copied, and began searching Smith's phone without a warrant at the border in order to further non-border related investigations of other government agencies -- to Magistrate Judge Aaron.

The Second Circuit has previously applied the good faith exception in similar circumstances to these. In United States v. Thomas, 757 F.2d 1359 (2d Cir. 1985), DEA agents used a dog to smell directly outside a suspect's apartment to determine whether drugs were inside. Id. at 1366. Based in significant part on the results of this "canine sniff," the Government applied for and obtained a search warrant to search the suspect's home. Id. The Second Circuit agreed with the defendant that the initial canine sniff was itself an unconstitutional search, conducted without a warrant or probable cause. Id. at 1366-67. It further agreed that -- without the results of the unconstitutional canine sniff -- there was no probable cause to search the defendant's home, such that no search warrant should have issued. Id. at 1367-68. But, notwithstanding that determination, the Second Circuit concluded that suppression would be inappropriate, because the Government "brought [its] evidence, including the positive 'alert' from the canine, to a neutral and detached magistrate," and "[t]hat magistrate determined that probable cause to search existed, and issued a search warrant." Id. at 1368. Since "[t]he magistrate, whose duty it is to interpret the law, determined that the canine sniff could form the basis for probable cause[,] it was reasonable for the officer to rely on this determination." Id.

This is not to say a later-issued warrant that relies for probable cause on unconstitutionally obtained information always suffices to establish good faith. Where law enforcement agents fail to disclose relevant facts to the magistrate, or have independent reason to know

their actions were unconstitutional, then a later obtained search warrant will not automatically establish good faith. See United States v. Reilly, 76 F.3d 1271, 1281 (2d Cir. 1996). But where "the issuing magistrate was apprised of the relevant conduct, so that the magistrate was able to determine whether any predicate illegality precluded issuance of the warrant . . . invoking the good faith doctrine does not launder the agents' prior unconstitutional behavior . . . [and instead] reaffirms Leon's basic lesson: that suppression is inappropriate where reliance on a warrant was objectively reasonable." United States v. Galias, 824 F.3d 199, 223 (2d Cir. 2016) (en banc).

That precisely describes the situation here. There is no suggestion that government agents concealed any relevant facts from Magistrate Judge Aaron. To the contrary, they disclosed precisely those facts that now lead this Court to conclude the initial border search was unlawful in their application for a warrant. In nevertheless in issuing the warrant, the Magistrate Judge implicitly (if erroneously) found that the underlying border search that resulted in a copy of Smith's phone was lawful or, at the very least, that probable cause independent of that search existed to search the copy. Nor is this a case where law enforcement "could not fail to have known" that their search was unconstitutional. Reilly, 76 F.3d at 1281. Rather, like the law enforcement agents in Thomas, at the time of the search in this case, "no court in this Circuit had held that" phone searches

at the border "w[ere] unconstitutional." Ganias, 824 F.3d at 223.¹⁴ Since the unconstitutionality of the search of Smith's phone was not obvious and law enforcement agents presented all relevant facts that might (and, in this Court's view, do) establish its unconstitutionality to a neutral magistrate, their subsequent reliance on the search warrant issued by that magistrate was objectively reasonable.

That does not quite settle the question, because of the significant length of time -- 38 days -- between the Government's March 2, 2021 search and copying of Smith's phone and its finally obtaining a warrant on April 9, 2021. In general, if law enforcement seizes personal property before obtaining a warrant and seeks a warrant after the fact, it must act "with diligence [in] apply[ing] for the warrant." United States v. Smith, 967 F.3d 198, 205 (2d Cir. 2020). Law enforcement must act with "expediency in obtaining a search warrant to search seized evidence in order to avoid interfering with a continuing possessory interest for longer than reasonably necessary," and because "unnecessary delays [] undermine the criminal justice process in a more general way [by] prevent[ing] the judiciary from promptly evaluating and correcting improper seizures." Id. Here, however, Smith makes no argument concerning the length of the delay between the copying of his phone's contents on March 2 and the Government's obtaining a warrant for it on April 9, so the issue is

¹⁴ This was true both in the Second Circuit, where the warrant was requested, and in the Third Circuit where the earlier search took place.

plainly waived. And even if that were not the case, the Court would still conclude that the good faith exception entitles the Government to rely on the April warrant.

In determining whether a particular delay between a seizure and the issuance of a warrant is reasonable, the Second Circuit has held that courts should consider "the following four factors . . . [1] the length of the delay, [2] the importance of the seized property to the defendant, [3] whether the defendant had a reduced property interest in the seized item, and [4] the strength of the state's justification for the delay." Id. at 206. The Government's delay here was plainly significant, since the Second Circuit has already held that a one-month delay (which is slightly shorter than the delay at issue here) "well exceeds what is ordinarily reasonable." Id. at 206. However, unlike in the typical case of delay following a warrantless seizure, Smith was not actually deprived of his use of his phone or the data stored on it, since the Government returned the original to him after it copied its contents. That makes this a different case from the Second Circuit's decision in Smith, where the police had seized a suspect's iPad, thereby depriving its owner of its use. Id.

Moreover, as in Smith itself, finding that the Government waited too long to seek a warrant would not necessarily justify excluding the results of its post-warrant search of the seized contents. How to think about the storage of forensic copies of a device containing digital data -- and the extent of the intrusion on a person's privacy interests resulting from the storage of such copies -- is a relatively

novel question. In Ganias, the Second Circuit concluded that law enforcement acted in good faith where it obtained a warrant to seize and search a person's computer hard drives, made and retained forensic copies of the hard drives for several years, and ultimately searched those copies years later for information that was not responsive to the original warrant that led to the creation of the forensic copies. Ganias, 824 F.3d at 225. To be sure, there the Government was acting in reliance on a (years-earlier issued) warrant, id., whereas here the initial search and digital copying of the contents of Smith's phone was warrantless, but Ganias, which declined to settle whether the Government's actions violated the Fourth Amendment, emphasized the unsettled and evolving nature of the law when it comes to copying and preserving electronic copies of the data on an electronic device. Id. at 208-21.

Moreover, while the Second Circuit in Smith clarified that a month was too long to wait in order to seek a warrant for a previously seized electronic device no longer available to its owner, id., it did not address a situation such as the one here, where the Government returned the actual phone and kept and (for the most part) searched the electronic copy after the warrant was issued. As in Smith, therefore, the Court is "not convinced that an objectively reasonable officer would have known that the delay [in obtaining a warrant] amounted to a violation of the Fourth Amendment." 967 F.3d at 213.

Accordingly, for the foregoing reasons, the Court concludes that the good faith exception doubly applies here, so that while the

Government's initial warrantless search of Smith's phone was unlawful, the results of that search (alongside the subsequent wiretap) should not be suppressed. Smith's motion to suppress is therefore denied.

III. Smith's motion to dismiss

Smith also moves to dismiss the indictment, contending that the Government's prosecution of him and the other defendants in this case was discriminatory. Smith Mem. 13-15. In support, he notes that he is black, the other defendants charged in this case are all either black or brown skinned, and that the affidavits submitted in support of the Government's warrant and wiretap applications refer to putative connections between Smith and other defendants with the Bloods gang. Id.; Smith Decl. ¶¶ 8-15, Dkt. 160. Smith also contends that many EMS companies are owned by white men whom the Government has declined to prosecute. Smith Decl. ¶ 14-15.

Because prosecution decisions are the "special province of the Executive," a "presumption of regularity supports [its] prosecutorial decisions," such that "absen[t] clear evidence to the contrary, courts presume that they have properly discharged their official duties." United States v. Armstrong, 517 U.S. 456, 464 (1996). While that presumption may be overcome by evidence "that the decision whether to prosecute . . . [was] based on an unjustifiable standard such as race, religion, or other arbitrary classification," such evidence must be "clear" and demonstrate that the "prosecutorial policy had a discriminatory effect and . . . was motivated by a discriminatory purpose." Id. at 465-66. To establish a discriminatory effect based

on race, a defendant "must show that similarly situated individuals of a different race were not prosecuted." Id. at 465.

Smith plainly fails to make the requisite showing. Smith has alleged only in very general terms that "owners of [EMS companies] and the people who worked for them -- almost entirely white men" without any gang connection also "settled their differences . . . by using threats of violence, violent kickbacks, or other illegal conduct." Smith Decl. ¶ 14. But while the indictment in this case lays out quite detailed allegations about Smith and his co-defendants' participation in a criminal enterprise that sought, inter alia, to impose a system of rules and rotation upon other EMS companies and use force to enforce that system, Indictment ¶¶ 6-10, Dkt. 2, Smith has not come forward with actual evidence of similar conduct by similarly situated white industry participants whom the Government has declined to prosecute. Similarly, Smith's only evidence of discriminatory intent is that the warrant and wiretap applications in this case referred to his and other defendants' putative connections with Bloods, but membership in the Bloods is certainly not itself any kind of protected status, and Smith has not explained how the Government's references to his or other defendants' putative connections to the Bloods demonstrate discrimination based on race or some other protected status. Accordingly, Smith's motion to dismiss the indictment is denied.

IV. Sequan Jackson's Motion to Suppress

Defendant Sequan Jackson also moved to suppress the results of a Title III wiretap of his and Smith's phones. As with Smith's motions

to suppress and dismiss, the Court denied Jackson's motion by bottom-line order earlier this year. See Order, Dkt. 183.¹⁵

To obtain a Title III wiretap, the government must provide "a full and complete statement of the facts and circumstances relied upon by the application" to establish probable cause, and a "full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. §§ 2518(1) (b)-(c). These restrictions aim "to guarantee that wiretapping or bugging occur[] only when there is a genuine need for it and only to the extent that it is needed." Dalia v. United States, 441 U.S. 238, 250 (1979). They require any "affidavit offered in support of a wiretap warrant [to] provide some basis for concluding that less intrusive investigative procedures are not feasible." United States v. Lilla, 699 F.2d 99, 103 (2d Cir. 1983). At the same time, they do not require "that any particular investigative procedures be exhausted before a wiretap may be authorized." Id. at 104. Rather, "the statute only requires that the agents inform the authorizing judicial officer of the nature and progress of the investigation and of the difficulties inherent in the use of normal law enforcement methods." United States v. Diaz, 176 F.3d 52, 111 (2d Cir. 1999). The Second Circuit has previously indicated that wiretaps will often prove necessary "in

¹⁵ Jackson has since pled guilty to certain charges. See Order, Dkt. 202.

complex and sprawling criminal cases involving large conspiracies," given the difficulties to obtaining evidence in such cases. United States v. Concepcion, 579 F.3d 214, 218 (2d Cir. 2009).

Jackson's primary argument is that the Government failed to establish that normal investigative procedures failed, would not succeed, or were too dangerous. Jackson Mem. 19-25, Dkt. 140. For instance, although the Government clearly gleaned extensive information from witness interviews (much of which formed the basis for its assertion there was probable cause for a wiretap), Clark Wiretap App. at 20-26, Jackson argued that the Government essentially stopped interviewing witnesses following the approval of the wiretap in order "to create the appearance of necessity" for its extension. Jackson Mem. 20. But just because the Government was able to make significant initial progress in its investigation with witness interviews does not mean that it could have continued to do so. As the Government cogently explained in support of its wiretap application, while its extensive witness interviews provided "important information" about how the alleged scheme was enforced as to victims, "victims have limited insight into the internal operations of the racketeering scheme . . ." Clark Wiretap App. at 49. The Government further explained that because many of the victims it interviewed reasonably feared retaliation, their willingness to cooperate was often limited. Id. These explanations, along with the rest of the Government's wiretap explanation, more than satisfies the statutory requirement that the Government explain why further witness interviews

"reasonably appear[ed] to be unlikely to succeed" in obtaining further evidence. 18 § 2518(1) (c).¹⁶

Jackson also points out that the Government was aware from its search of Smith's phone that First Response members communicated through an end-to-end encrypted WhatsApp chat which would not itself be observable through a wiretap. As such, Jackson suggests, that the Government should have sought cooperation from one of the many people included on one of the WhatsApp chats. But the wiretap application explains that while the Government obtained some information from cooperating witnesses, it was not aware of further confidential sources whom it believed would have relevant information and be willing to work with the Government. Clark Wiretap App. at 42-43. Of course, as Jackson notes, the Government could presumably have approached one of the participants in the WhatsApp group chats -- but such a move could just as easily have resulted in that participant tipping off Smith,

¹⁶ Jackson also suggests that because the Government has provided Jencks Act material for over 40 witnesses, it ultimately was able to obtain evidence from substantially more witnesses than the 16 it interviewed when applying for a wiretap -- indicating that there was more to be gained from witness interviews. Jackson Mem. 20-21. The Court is not convinced. For one thing, the fact that the Government produced Jencks Act evidence for more witnesses than it had apparently interviewed before seeking a wiretap does not itself raise any inference as to the quality of information provided by the additional witnesses. Furthermore, the wiretap itself likely produced new lines of inquiry, and the Government represents that additional witnesses became willing to speak to law enforcement after the charges in this case were brought. Gov't Mem. 23 n.3, Dkt. 164. So the fact that the Government ultimately interviewed more witnesses hardly defeats its explanation as to why, at the time it sought a wiretap, it was unlikely to obtain the information it needed from further witness interviews alone.

Jackson, or the other targets of the investigation. Gov't Mem. at 23-24. Similarly, Jackson speculates that an undercover agent could potentially have gained access to the WhatsApp chats or otherwise obtained valuable information by appearing at the site of a fire and seeking to "blend" in with individuals from First Response as they showed up, Jackson Mem. 22, but that is pure speculation that would require undercover agents to show up at a moment's notice at the site of a fire, identify if EMS personnel who showed up were connected with First Response, and then somehow insinuate themselves into those persons' conversations. Such a speculative possibility is not enough to preclude issuance of a wiretap.¹⁷

The Court is similarly unpersuaded that there was anything deficient in the Government's representation in its warrant application that further physical surveillance would be insufficient, given the Government's description of its previous unsuccessful efforts to surveil the First Response office and monitor areas frequented by Smith and its explanation that because violence "occur[ed] at the site of fires or at other random locations," there

¹⁷ Jackson also implies that the Government's warrant application may not have been accurate because it describes an undercover HSI officer being sent to the scene of a fire in February 2021, Clark Wiretap Appl. at 41, even though the investigation that ultimately resulted in these charges was not formally opened until March 2021, id. at 14. Jackson Mem. 22 (arguing that "[t]his discrepancy raises the specter that there was, in fact, no actual use of an undercover officer"). But the Government explains that there were two overlapping investigations, and the February 2021 visit to the scene of a fire was conducted by officers associated with the earlier one. Gov't Mem. 26 n.5

was no practicable way to obtain needed evidence through physical surveillance. Clark Wiretap Application at 42-45.

Finally, Jackson argues that the wiretap never should have been approved because the Government knew from its search of Smith's phone that most of his text communications were sent by WhatsApp, and the Government's wiretapping technology allegedly would not allow it to pierce WhatsApp's end-to-end encryption. Jackson Mem. at 25-27. The Court is not persuaded. The fact that the majority of Smith's written messaging with large groups was through WhatsApp does not imply he used WhatsApp to make phone calls, and, indeed, the Government's wiretap application detailed several phone calls placed between Smith's cell phone and other suspects. Clark Wiretap App. at 38-41. Accordingly, the fact that Smith employed WhatsApp messaging did not mean the Government lacked reason to expect it would obtain valuable information from a wiretap.

The Court thus agrees with Judge Liman's determination that the Government adequately demonstrated that other investigative methods were not reasonably likely to succeed and that a wiretap was therefore necessary. Accordingly, Jackson's motion to suppress is denied.

V. Defendants' Dore and Lacewell's Motion to Sever

Finally, defendants Damon Dore and Rahmiek Lacewell moved under Fed. R. Crim. Proc. 14 to sever their trial from Jatiek Smith's.¹⁸

¹⁸ Defendant Sequan Jackson originally joined this motion, although he subsequently withdrew from it. Dkt. 169. The motion was also joined by defendants Anthony McGee and Kaheen Small, who entered guilty pleas before the Court denied the motion. See Minute Entries

They argued that certain inculpatory evidence obtained during an interview Smith gave law enforcement might be admissible as to Smith but inadmissible as against them, that Smith is the most culpable of any defendant, and that Smith's pretrial behavior indicates he is likely to behave in a way during trial that will prejudice a jury against not just him but also moving defendants. See generally Mem. Supp. Mot. Sever, Dkt. 144. None of these arguments merit severance.

"A trial court has wide discretion in considering a motion to sever under Federal Rule of Criminal Procedure 14." United States v. Gallo, 863 F.2d 185, 194 (2d Cir. 1988); see Zafiro v. United States, 506 U.S. 534, 539 (1993). To succeed on a motion to sever, the defendant must demonstrate "substantial prejudice," United States v. Werner, 620 F.2d 922, 928 (2d Cir. 1980), such as might occur when evidence that would not be admissible as against the defendant seeking severance would be admissible against another and the evidence is of a sort that limiting instructions seem unlikely to cure any prejudice. Zafiro, 506 U.S at 539.

As to Smith's inculpatory statements, the Government argues that such statements are admissible against all defendants as co-conspirator statements, since, the Government contends, Smith gave the interview in question in order "to thwart law enforcement's investigation into those crimes by deflecting law enforcement's

dated 3/6/23 and 3/14/23. Lacewell and Dore have also subsequently pled guilty, although their pleas came after the Court denied their motion to sever by bottom-line order. See Order, Dkt. 183.

attention away from First Response and onto other EMS companies." Gov't Mem. at 13, Dkt. 164. The Court sees no need to resolve whether these statements really would have been admissible against defendants other than Smith for two reasons. First, even assuming moving defendants were right that these statements would be admissible against Smith but not them, they have not pointed to any statements that would be so likely prejudicial that an appropriate limiting instruction would not adequately address their concerns. Further, the Government represents it has not even decided whether to seek to introduce any of these statements at trial, and that it would first resolve their admissibility via a motion in limine if it does choose to seek to introduce them.

As to defendants' argument that Smith is the most culpable defendant, the charges here -- racketeering and extortion conspiracy -- necessarily involve the actions of multiple individuals, with some likely more culpable than others. The Government represents that the evidence it intends to rely on to prove each defendant's participation in the conspiracy substantially overlaps. Even if moving defendants are right that their participation was less culpable than Smith's, the Court does not believe that such differential culpability does not by itself merits severance, absent some more particular showing that a joint trial is likely to prejudice a jury against moving defendants.

Finally, defendants' arguments about Smith's potential disruptiveness at trial are entirely speculative. They are based entirely on Smith's conduct in resisting arrest and in his refusal to

leave a court cell block and return to jail following a conference earlier in this case. Defs. Mem. at 12, Dkt. 144. Mr. Smith has appeared at several court conferences and behaved in all respects appropriately while in Court; his apparent resistance to being returned to jail after one of these court appearances does not demonstrate that Smith will behave at trial in a way likely to cause prejudice to other defendants (especially since Smith himself will have every incentive at trial to present himself favorably to the jury). Accordingly, defendants Dore and Lacewell's motion to sever is denied.

VI. Conclusion

For the foregoing reasons, as indicated in its previous bottom-line order, the Court hereby reconfirms its denial of defendant Jatiek Smith's motion to suppress the results of the search of his phone and to dismiss the indictment, defendant Sequan Jackson's motion to suppress evidence obtained from Title III wiretaps, and defendants Dore and Lacewell's motion to sever their trial from Smith's.

SO ORDERED.

New York, NY
May 16, 2023



JED S. RAKOFF, U.S.D.J.